STATE OF CALIFORNIA—OFFICE OF ADMINISTRATIVE LAW

NOTICE PUBLICATION/REGULATION SUBMISSION

FILE PRINT

(See instructions on reverse)

STD. 400 (REV. 01-09)

For use by Secretary of State only

OAL FILE NUMBERS	NOTICE FILE NUMBER	REGULATORY ACTION NUMBER	EMERGENCY NUMBER
	Z-	2011-1223-04FP	

For use by Office of Administrative Law (OAL) only

2011 DEC 23 PM 12:13

OFFICE OF ADMINISTRATIVE LAW

NOTICE | REGULATIONS

ENDORSED - FILED
in the office of the Secretary of State
of the State of California
JAN 31 2012 3:01 PM
DEBRA BOWEN
Secretary of State

AGENCY WITH RULEMAKING AUTHORITY: California Health and Human Services Agency - Office of Health Information Integrity

AGENCY FILE NUMBER (If any):

A. PUBLICATION OF NOTICE (Complete for publication in Notice Register)

1. SUBJECT OF NOTICE	TITLE(S)	FIRST SECTION AFFECTED	2. REQUESTED PUBLICATION DATE

3. NOTICE TYPE	4. AGENCY CONTACT PERSON	TELEPHONE NUMBER	FAX NUMBER (Optional)
☐ Notice re Proposed Regulatory Action ☐ Other			

OAL USE ONLY — ACTION ON PROPOSED NOTICE	NOTICE REGISTER NUMBER	PUBLICATION DATE
☐ Approved as Submitted ☐ Approved as Modified ☐ Disapproved/ Withdrawn		

B. SUBMISSION OF REGULATIONS (Complete when submitting regulations)

1a. SUBJECT OF REGULATION(S)	1b. ALL PREVIOUS RELATED OAL REGULATORY ACTION NUMBER(S)
HIE Demonstration Project Regulations	N/A

2. SPECIFY CALIFORNIA CODE OF REGULATIONS TITLE(S) AND SECTION(S) **(Including title 26, if toxics related)**

SECTION(S) AFFECTED (List all section number(s) individually. Attach additional sheet if needed.)	
	ADOPT: 126010, 126020, 126030, 126040, 126042, 126050, 126055, 126060, 126070, 126072, 126074, 126076, 126090
	AMEND:
TITLE(S): 22	REPEAL:

3. TYPE OF FILING

- ☐ Regular Rulemaking (Gov. Code §11346)
- ☐ Resubmittal of disapproved or withdrawn nonemergency filing (Gov. Code §§11349.3, 11349.4)
- ☐ Emergency (Gov. Code, §11346.1(b))
- ☐ Certificate of Compliance: The agency officer named below certifies that this agency complied with the provisions of Gov. Code §§11346.2-11347.3 either before the emergency regulation was adopted or within the time period required by statute.
- ☐ Resubmittal of disapproved or withdrawn emergency filing (Gov. Code, §11346.1)
- ☐ Emergency Readopt (Gov. Code, §11346.1(h))
- ☒ File & Print
- ☐ Other (Specify) _____
- ☐ Changes Without Regulatory Effect (Cal. Code Regs., title 1, §100)
- ☐ Print Only

4. ALL BEGINNING AND ENDING DATES OF AVAILABILITY OF MODIFIED REGULATIONS AND/OR MATERIAL ADDED TO THE RULEMAKING FILE (Cal. Code Regs. title 1, §44 and Gov. Code §11347.1)

5. EFFECTIVE DATE OF CHANGES (Gov. Code, §§ 11343.4, 11346.1(d); Cal. Code Regs., title 1, §100)

- ☐ Effective 30th day after filing with Secretary of State
- ☒ Effective on filing with Secretary of State
- ☐ §100 Changes Without Regulatory Effect
- ☐ Effective other (Specify) _____

6. CHECK IF THESE REGULATIONS REQUIRE NOTICE TO, OR REVIEW, CONSULTATION, APPROVAL OR CONCURRENCE BY, ANOTHER AGENCY OR ENTITY

- ☐ Department of Finance (Form STD. 399) (SAM §6660)
- ☐ Fair Political Practices Commission
- ☐ State Fire Marshal
- ☐ Other (Specify) _____

7. CONTACT PERSON	TELEPHONE NUMBER	FAX NUMBER (Optional)	E-MAIL ADDRESS (Optional)
Alex Kam	(916) 654-2873	(916) 653-9588	akam@ohi.ca.gov

8. **I certify that the attached copy of the regulation(s) is a true and correct copy of the regulation(s) identified on this form, that the information specified on this form is true and correct, and that I am the head of the agency taking this action, or a designee of the head of the agency, and am authorized to make this certification.**

SIGNATURE OF AGENCY HEAD OR DESIGNEE: [signature] DATE: 12/23/11

TYPED NAME AND TITLE OF SIGNATORY: Alexander Kam, Acting Director

For use by Office of Administrative Law (OAL) only

ENDORSED APPROVED
JAN 31 2012
Office of Administrative Law

Title 22, Division 14
California Office of Health Information Integrity

Table of Contents

§126010	Applicability of Regulations	2
§126020	Definitions	2
§126030	California Health Information Exchange Practices Principles	5
§126040	Transparency and Complaint Process	6
§126042	Trade Secret Designation and Protections	7
§126050	Permitted Purposes for Exchanging Health Information	9
§126055	Informing Requirements; Affirmative Consent; Revocation of Consent	9
§126060	Requests to Develop Alternative Requirements	11
§126070	Security Requirements – General	13
§126072	Security Requirements – Administrative Controls	13
§126074	Security Requirements – Physical Controls	14
§126076	Security Requirements – Technical Controls	15
§126090	Demonstration Projects Oversight	16

ALL NEW TEXT

Title 22, Division 14 California Office of Health Information Integrity

Chapter 1: Demonstration Projects for the Electronic Exchange of Health Information

§126010 Applicability of Regulations

(a) The regulations in this chapter apply to demonstration project Applicants and Demonstration Project Participants as defined in California Health and Safety Code §130276.

(b) Effective dates. The regulations adopted in this chapter will become inoperative on the date the CalOHII Director executes a declaration stating that the grant period for the State Cooperative Grant Agreement for health information exchange has ended and this chapter will then be repealed.

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: California Health and Safety Code §§ 130276, 130277,130278, 130282.

§126020 Definitions

(a) "Access" means the HIPAA definition given at 45 C.F.R. §164.304.

(b) "Affiliated organization" means legally separate organizations which have designated themselves as a single, affiliated organization and are under common ownership or control or are a part of the same Organized Health Care Arrangement ("OHCA") as defined by HIPAA.

(c) "Applicant" means an entity that submits an application to CalOHII for approval as a demonstration project.

(d) "Authorization" as used in section 126055(b)(2) means written permission in the form required for compliance with Civil Code sections 56.11, 56.21; Insurance Code section 791.06, and/or 45 C.F.R. §164.508 or as required by more stringent law as defined by 45 CFR §160.202.

(e) "Business Associate" means the HIPAA definition given at 45 C.F.R. §160.103.

(f) "CalOHII" means the California Office of Health Information Integrity.

(g) "CMIA Provider" means the Confidentiality of Medical Information Act definition of a Provider of Health Care given at Civil Code section 56.05(j).

(h) "De-identified health information" means the HIPAA definition given at 45 C.F.R. §164.514.

(i) "Demonstration Project Participant" means any provider, health plan, health information organization, or governmental authority approved by CalOHII to test privacy and/or security policies for the exchange of electronic health information in the demonstration project.

(j) "Disclosure" means the HIPAA definition given at 45 C.F.R. §160.103.

(k) "Electronic Health Record (EHR)" means the definition given at section 13400 of subtitle D of the American Recovery and Reinvestment Act of 2009: "an electronic record of health-related information about an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff."

(l) "Governmental authority" means any municipal, county, state or other governmental entity that has jurisdiction and control over the provision or payment for medical services or that routinely received medical information to complete its designated governmental function, including specialized units from the local and state public health authorities.

(m) "Health Care Provider" means the HIPAA definition given at 45 C.F.R. §164.103.

(n) "Health Information Organization" (HIO) means a third party facilitator that conducts, oversees, or governs the disclosure of individual health information among separate, unaffiliated entities.

(o) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996 as amended by subsequent legislation and the implementation of Privacy, Security, and Enforcement Rules under 45 C.F.R. Part 160 and Subparts A, C, D, and E of Part 164.

(p) "HIPAA covered entity" means the HIPAA definition for covered entity given at 45 C.F.R. 160.103.

(q) "Independent Directed Exchange" means the electronic disclosure of encrypted individual health information over the internet to an unaffiliated entity and where third party facilitators do not have the ability to decrypt the content of the individual health information (IHI) package nor provide governance or oversight.

(r) "Individual" means the person who is the subject of health information.

(s) "Individual Health Information" (IHI) means information, in oral, electronic or physical form, including demographic information collected from an individual, and:

(1) Is created or received by or derived from a health care provider, health care clearinghouse, health plan, employer, pharmaceutical company, or contractor;
(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
(3) Is Individually identifiable which means the information includes or contains any element of personal identifying information to which there is a reasonable basis to believe the information can be used to identify the individual such as the patient's name, address, electronic mail address, telephone number, social security number, or other information that, alone or in combination with other potentially available information, reveals the individual's identity.

(t) "More stringent law" means: in the context of a comparison of a provision of state or federal law, including HIPAA, against another law, a "more stringent law" is one that meets one or more of the following criteria:

(1) With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted under another law or rule, except if the disclosure is
  (A) Required by the federal Secretary of Health and Human Services in the context of HIPAA, in connection with determining whether a covered entity is in compliance with this subchapter; or
  (B) To the individual who is the subject of the individual health information.

(2) With respect to the rights of an individual, who is the subject of the individual health information, regarding access to or amendment of individual health information, permits greater rights of access or amendment, as applicable.

(3) With respect to information to be provided to an individual who is the subject of the individual health information about a use, a disclosure, rights, and remedies, provides the greater amount of information.

(4) With respect to the form, substance, or the need for express legal permission from an individual, who is the subject of the individual health information, for use or disclosure of individual health information, provides requirements that narrow the scope or duration, increase the privacy protections afforded (such as by expanding the criteria for), or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable.

(5) With respect to recordkeeping or requirements relating to accounting of disclosures, provides for the retention or reporting of more detailed information or for a longer duration.

(6) With respect to any other matter, provides greater privacy protection for the individual who is the subject of the individual health information.

(u) "Participants Agreement" (PA) means a multi-party trust agreement among organizations exchanging health information that sets a common set of terms and conditions for the organizations establishing a mutual governance process amongst participants.

(v) "Public Health" This term refers to public health authorities whose public health programs promote, maintain, and conserve the public's health by providing health services to individuals and/or by conducting research, investigations, examinations, training, and demonstrations.

(w) "Sensitive health information" means legally established categories of sensitive information, such as genetic information, mental health, substance abuse treatment, HIV-related information, sexuality and reproductive health or specific segments of a patients individual health information for which a patient has requested protection from disclosure in writing.

(x) "Treatment" means the HIPAA definition given at 45 C.F.R. §160.103.

(y) "Use" means the HIPAA definition given at 45 C.F.R. §160.103.

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: California Civil Code§§ 56.05, 56.06; Health and Safety Code §§ 130200, 130201, 130276, 130277, 130278; 45 C.F.R. §§160.103, 164.304, 164.501.

§126030 California Health Information Exchange Practices Principles

(a) Demonstration Project Participants shall adhere to the following principles of fair information practices:

(1) Openness – There should be a general policy of openness among entities that participate in electronic health information exchange about developments, practices, and policies with respect to individual health information.

(2) Individual Health Information Quality – Health information shall be relevant, accurate, complete, and kept up-to-date.

(3) Individual Participation – Individuals or their personal representatives have the right to:

(A) Ascertain the person responsible for individual health information for an entity, obtain confirmation of whether the entity has specific individual health information relating to the individual, and obtain its location.

(B) Receive their individual health information in a reasonable time and manner, at a reasonable charge, and in a format that is generally accessible by individuals.

(C) Challenge the accuracy of their individual health information and, if successful, to have the individual health information corrected, completed, or amended.

(D) Control the access, use, or disclosure of their individual health information, unless otherwise specified by law or regulation.

(4) Collection Limitation – There shall be limits to the collection of individual health information. Individual health information shall be obtained by lawful and fair means. Where appropriate, it shall be obtained with the knowledge or consent of the individual or their personal representative. The specific purposes for which individual health information is collected shall be specified not later than at the time of collection.

(5) Individual Health Information Limitation – Use and disclosure of individual health information shall be limited to the specified purpose. Certain use and disclosure shall require consent.

(6) Purpose Limitation – Individual health information shall be relevant to the purpose for which it is to be used and, limited to the minimum information necessary for the specified purpose. The subsequent use shall be limited to the specified purpose.

(7) De-Identified Information – De-identified individual health information shall not be re-identified unless specified in law. If de-identified individual health information is re-identified, it shall be subject to these principles. De-identified

individual health information shall not be disclosed if there is a reasonable basis to believe that the information can be used to identify an individual.

(8) Security Safeguards – Individual health information should be protected by appropriate security safeguards against such risks as loss or destruction, unauthorized access, use, modification or disclosure of data.

(9) Accountability – An entity shall comply with laws, regulations, standards and organizational policies for the protection, retention and destruction of individual health information. Any person who has access to individual health information shall comply with those provisions.

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: Health and Safety Code §§ 130200, 130277, 130279.

§126040 Transparency and Complaint Process

(a) Prior to the approval of any demonstration project, the Applicant must provide CalOHII with copies of:
  (1) The Applicant's Notice of Privacy Practices created pursuant to 45 C.F.R. §164.520.
  (2) The Applicant's Participants Agreement and a list of the entities included in the agreement.
  (3) A description of the Applicant's complaint mechanism required by §126040(d), including any documentation or patient educational materials related to the complaint process.

(b) Once a demonstration project is approved, but prior to the start of the demonstration project, within a specified time frame negotiated with and approved by CalOHII, the Demonstration Project Participant must provide:

  (1) If the Demonstration Project Participant is a HIO, a list of all parties who have signed the HIO's Participant Agreement, with their contact information and a general description of the service(s) provided, including the data shared, the purpose, and whether further dissemination of the data is allowed, regardless of whether the information is de-identified.

  (2) If the Demonstration Project Participant is not a HIO, a list of all of the Participant's current business associates with electronic access to individual health information disclosed through the demonstration project, with their contact information and a general description of the service(s) provided, including the data shared, the purpose, and whether further dissemination of the data is allowed, regardless of whether the information is de-identified.

  (3) If a new business associate is added after the start of the project, or a business associate agreement is modified, the Demonstration Project Participant must provide CalOHII with an updated list quarterly.

  (4) In CalOHII's discretion, CalOHII may require copies of the Demonstration Project Participant's business associate agreements be provided to CalOHII. The

Participant shall provide copies within five working days from the receipt of written request from CalOHII.

(c) All unauthorized electronic disclosures or access of individual health information shall be reported by the Demonstration Project Participant to CalOHII within thirty (30) business days of the detection of the unauthorized access or disclosure. Good faith acquisition of IHI by an employee or agent within the course of coordinating care or delivering treatment services, provided that IHI is not used or subject to further unauthorized disclosure do not need to be reported. A report to CalOHII under this provision does not relieve the Demonstration Project Participant from any requirement under any local, state, or federal law.

(d) A Demonstration Project Participant must ensure there is a mechanism to receive and respond to patient complaints.

(1) Complaints associated with the demonstration project shall be reported and forwarded to CalOHII quarterly and include the Demonstration Project Participant's response to any complaint regarding the demonstration project.

(2) Complaints reflecting significant risk to patient privacy and confidentiality of individual health information or patient health and safety attributable to the demonstration project shall be reported by the Demonstration Project Participant to CalOHII immediately.

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: Health and Safety Code §§ 130200, 130277, 130279.

§126042 Trade Secret Designation and Protections

(a) All of the information provided to CalOHII by Demonstration Project Applicant or Participant shall be treated as a public record unless such information is designated to be a trade secret or unless the public interest in maintaining the confidentiality of that information clearly outweighs the public interest in disclosure.

(1) Any records, or portion thereof, which the Demonstration Project Applicant/Participant wants to protect as a trade secret shall be submitted in a separate sealed envelope clearly marked on the outside as "Trade Secret Material." For purposes of this section, "trade secret" shall have the same meaning as in the Uniform Trade Secrets Act, *Civil Code section 3426* et seq. The Application shall contain a declaration under penalty of perjury describing why the Applicant/Participant believes the material is a trade secret. After review, if CalOHII determines that the material submitted meets the definition of a "trade secret", then CalOHII will treat the material as such and will exempt it from disclosure. If it is determined that the material does not meet the definition of a "trade secret", then the material or information will be disclosed as public information in accordance with the Public Records Act, Government Code section 6250. CalOHII's refusal to grant a requested claim of trade secret does not excuse the Applicant from establishing all elements of the demonstration project application. Any material which CalOHII agrees to consider as a trade secret shall be exempt from disclosure under the Public Records Act, *Government Code*

section 6250 et seq. Records for which CalOHII has denied protection as a trade secret shall also be exempt from disclosure under the Public Records Act during the time the records are in the possession of CalOHII.

(2) The Demonstration Project Applicant/Participant shall have the sole burden of designating, at the time of its submission, any specific information that it believes should be treated as confidential and the reasons therefore.

(b) Requests for Confidentiality. A request for confidential treatment of any information received in connection with any demonstration project application or report submitted to CalOHII must accompany the submission of such information. The confidential information must be submitted separated from the other parts of the filing and marked "Confidential Treatment Requested." The request for confidentiality should not contain confidential information, as requests for confidentiality will be available for public inspection. Confidential Treatment Requests must be signed by the person making the application or report and contain the following:

(1) A statement identifying the information which is the subject of the request, the application or report it relates to, and a reference that the request is made pursuant to this provision.

(2) A statement of the grounds upon which the request is made, including (if applicable) a statement as to its confidentiality and the measures taken to protect its confidentiality, and a statement of the adverse consequences which are expected to result if the information is disclosed through the public records of CalOHII.

(3) A statement of the specific time for which confidential treatment of the information is necessary and the basis for such conclusion.

(4) If appropriate, a statement of the extent to which such information has been previously disclosed or will be disclosed in the future.

(c) Granting of Request. If a request for confidential treatment is granted, the person making such request will be notified in writing, the information will be marked "confidential" and kept separate from the public file, and the application or report will be noted with the following legend: "Additional portions of this filing have been granted confidential treatment pursuant to Section 126042 and are contained in a separate confidential file."

(d) Information contained in confidential files shall only be disclosed to authorized representatives of the Demonstration Project Applicant/Participant or other governmental agencies as necessary for them to perform their constitutional or statutory duties or as required by law.

(e) In the event of a receipt of a subpoena request for designated confidential materials, before the disclosure, CalOHII will make a reasonable attempt to notify the submitter of the information before the mandated disclosure, if the notification is not prohibited by law.

Authority: California Health and Safety Code §§ 130277, 130278.

Reference: Civil Code § 3426; Government Code § 6250 et seq.; California Health and Safety Code §§ 130276, 130277,130278, 130282.

§126050 Permitted Purposes for Exchanging Health Information

(a) Permitted purposes. The Demonstration Project Participants that discloses individual health information through a HIO or an independent directed exchange, or uses individual health information in an affiliated organization shall be limited to:

(1) Treatment.

(2) Reporting to Public Health Officials for immunizations, bio-surveillance and mandated reporting.

(3) Quality reporting for meaningful use to Centers for Medicare and Medicaid Services and the California Department of Health Care Services.

(4) HIPAA mandated transactions consistent with 45 C.F.R . §162.900 through 45 C.F.R. §162.1802 for transaction standards and code sets.

(b) Permitted secondary purposes. Participants in the demonstration project may use or disclose individual health information after it is disclosed through a HIO, affiliated organization, or independent directed exchange for any permitted purpose allowed by law and/or that is specified in the Demonstration Project Participant's Notice of Privacy Practices created in accordance with 45 C.F.R. §164.520.

(c) These provisions do not apply to business practices that use electronic faxes or emails.

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: Health and Safety Code §§ 130200, 130277, 130279; 45 C.F.R. §162.923, §164.520.

§126055 Informing Requirements; Affirmative Consent; Revocation of Consent

(a) Informing Requirements

(1) Prior to requesting consent from an individual or the individual's legally authorized personal representative to permit the electronic exchange of health information among separate, unaffiliated entities, Demonstration Project Participant shall provide notice to the individual or the individual's legally authorized personal representative, which at a minimum shall contain statements describing:

(A) Electronic exchange of health information.

(B) Uses of IHI, which may incorporate the Demonstration Project Participant's Notice of Privacy Practices created in accordance with 45 C.F.R. §164.520, if appropriate.

(C) Benefits and risks associated with disclosing IHI through a HIO or independent directed exchange, including the exchange of sensitive health information, such as HIV status, mental health records, reproductive health records, drug and alcohol treatment records, and genetic information which

could be inferred or embedded in information that is made available through a HIO or independent directed exchange.

(D) Consent requirements.

(E) Specific exceptions to the consent requirements for electronic exchange of health information for mandated public health reporting and for transmitting mandated HIPAA transactions and code sets.

(F) Specific exceptions to the consent requirements in emergency situations.

(G) Process for revoking consent, including a contact name, phone number, email address, and website.

(H) When the revocation of consent is effective.

(b) Affirmative Consent

(1) Before an individual's individual health information is electronically disclosed through a HIO or independent directed exchange, Demonstration Project Participant shall obtain written affirmative consent documenting the individual's or the individual's legally authorized personal representative's choice to electronically disclose the individual's individual health information or verify the individual's consent in a centralized consent registry.

(2) Obtaining affirmative consent documenting the individual's or the individual's legally authorized personal representative's choice to electronically exchange their individual health information under this regulation does not necessarily relieve the Demonstration Project Participant from obtaining other legally required authorizations to disclose health information if other laws impose additional or different requirements that are not satisfied in the consent obtained pursuant to this regulation.

(3) Emergency situations

(A) A Demonstration Project Participant may disclose to a CMIA provider an individuals' health information through a HIO or independent directed exchange when:

i. The individual requires emergent care;
ii. The individual or the individual's legally authorized personal representative is incapable of consenting;
iii. The individual or the individual's legally authorized personal representative has not explicitly denied or withdrawn consent on a previous occasion; and
iv. It is in the best interest of the individual, as determined by the treating health care provider.

(4) Mandated public health reporting. Affirmative consent is not required for mandated public health reporting disclosures.

(5) Mandated HIPAA transactions and code sets. Affirmative consent is not required for mandated HIPAA transactions and code sets.

(c) Revocation of consent

(1) An individual or the individual's legally authorized personal representative may revoke their previously granted consent to the electronic exchange of health information among separate, unaffiliated entities by contacting the designated contact person or Demonstration Project Participant as described in the informing requirements in section (a).

(2) After the effective date of the revocation of consent, the Demonstration Project Participant shall not allow the individual's health information to be disclosed through a HIO or independent directed exchange unless and until the individual or the individual's legally authorized personal representative reinstates consent.

(d) An individual may re-establish consent at any time by providing written affirmative consent to the Demonstration Project Participant.

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: Health and Safety Code §§ 130200, 130277, 130279.

§126060 Requests to Develop Alternative Requirements

(a) An Applicant may request to demonstrate an alternative requirement from those stated in sections 126050, 126055, 126070, 126072, 126074, and 126076, if the Applicant is currently unable to comply with the requirement or has an alternative policy that it wants to test. All requests to develop alternative requirements must be submitted to CalOHII in writing, and include:

(1) The reason for the request.

(2) All supporting documentation, such as:

(A) If the reason is related to implementation delays, state the timeframe in which the requirement will be implemented.

(B) A description of, and copies of:

(i) Alternate privacy and security provisions that would provide similarly adequate compliance with the California Health Information Exchange Practices Principles,

(ii) Clear delineation of the purpose and the roles of those who may have access to the individual health information and any permitted subsequent use of the information, and

(iii) Information on the governance structure and evaluation of security compliance.

(b) In granting requests to develop alternative requirements, CalOHII will consider, but is not limited to the following factors:

(1) General factors:

(A) The proposal will advance the knowledge and development of privacy and security standards in a new area;

(B) Alternative requirements can provide similar compliance with the principles, without jeopardizing privacy and security of IHI;

(C) Patient safety concerns are significant;

(D) The technology is not readily available; and/or

(E) Insufficient benefit to individual privacy interests as compared to the costs or other legitimate burdens that would be incurred.

(2) Purpose limitations requirements in §126050

(A) The purpose is consistent with State law and not preempted by HIPAA;

(B) The Applicant can demonstrate adequate oversight to ensure no further disclosure or use of IHI unless the secondary use is consistent with the Civil Code sections 56.10, 56.13, 56.30 and more stringent laws; and

(C) If de-identified data is being used or generated, the recipients of the data are known.

(3) Informing and Consent requirements in §126055

(A) For HIO and independent directed exchanges of IHI:

(i) The circumstances ensure that patients or their representatives are made aware that IHI is being disclosed, to whom and for what purpose, and whether they have the right to refuse and if they so choose the option to not permit their health information to be disclosed, what are the possible consequences to them;

(ii) The data being disclosed, whether it is considered sensitive health information, and whether the disclosure is narrowly tailored to the need for the information.

(B) For independent directed exchanges, in addition to paragraph (A):

(i) The disclosure is made to another CMIA provider;

(ii) The disclosure is by means of a secure transaction;

(iii) The other CMIA provider has a current treating relationship with the patient;

(iv) The disclosure does not contain sensitive health information nor is the information about another individual; and

(vi) There is no re-purposing or re-directing of the information.

(4) Security Controls requirements in §126070-126076

(A) Adequacy of the alternative security controls in addressing the particular circumstance; and

(B) Whether the proposed security provision is consistent with a mandatory HIPAA provision.

(c) CalOHII shall document in writing each grant of a request to demonstrate an alternative requirement within forty-five (45) days of the receipt of the DAR at CalOHII, and will make the request and a summary of the basis for the decision publicly available.

(1) In cases where a DAR is submitted with insufficient information for CalOHII to determine approval, a 15 day extension period may be provided to CalOHII to collect information and documentation in order to make a determination.

Authority: California Health and Safety Code §§ 130277, 130278.

Reference: Health and Safety Code §§ 130200, 130277, 130279.

§126070 Security Requirements – General

(a) All Demonstration Project Participants must:

(1) Protect the confidentiality, integrity, and availability of all electronic IHI the Demonstration Project Participant creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under California law.

(4) Monitor compliance with these requirements by the Demonstration Project Participant's workforce. (b) All Demonstration Project Participants and any recipient of IHI received in a demonstration project, who are a HIPAA covered entity or a business associate of a HIPAA covered entity, are required to comply with the HIPAA security standards in Subpart C of Part 164, 45 C.F.R. §164.302 et seq, with respect to the IHI and any risk assessment must include an evaluation of the additional risk incurred by being a Participant in an exchange of health information.

Authority: California Health and Safety Code §§ 130277, 130278.

Reference: California Civil Code§§ 56.13, 1798.21, 1798.81.5; Health and Safety Code §§ 130200, 130277, 130279; 45 C.F.R. §§ 164.302, 164.306(a)

§126072 Security Requirements – Administrative Controls

(a) Access Controls. A Demonstration Project Participant shall utilize identity management, authentication, and authorization mechanisms to ensure that only authorized users have access to information systems.

(1) Identity Management (Internal). A Demonstration Project Participant shall establish policies and procedures to verify the identity of workforce members who will access the-Participant's systems. A Demonstration Project Participant shall, at a minimum:

(A) Verify that the individual is the one claimed by examination of various forms of state-issued picture identifications such as a driver's license or ID card,

professional licenses in good standing from state or national certification boards, and other forms of identification issued by reliable bodies. The number and extent of such verification will be commensurate with the user's responsibilities and consistent with privileges they will be given (authorizations).

(B) Issue a user identifier and an identity certificate and/or token (password, hard token, soft cryptographic token or one-time password device tokens, etc.), to the verified person, as appropriate to their level of authorization.

(C) Be responsible for any health data access rights assigned to the authorized person based on their qualifications and role.

(D) Manage all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services.

(2) Single Entity Authentication (Non-Federated). A Demonstration Project Participant shall authenticate each authorized user's identity prior to providing access to IHI.

(A) A Demonstration Project Participant shall assign a unique name and/or number for identifying and tracking user identity and implement procedures to verify that a person or entity seeking access to IHI is the one claimed.

(B) A Demonstration Project Participant shall authenticate each user to the level of authorized access that complies with the Participant Agreement.

(C) A Demonstration Project Participant shall authenticate users attempting to access IHI from an unsecured location or device, shall require NIST Level 3 authentication in which the data requester must establish two factors of authentication. [See NIST SP 800-63 Rev-1]

Authority: California Health and Safety Code §§ 130277, 130278.

Reference: California Civil Code§§ 1798.20, 1798.21, 1798.81.5; Health and Safety Code §§ 1280.15, 130200, 130277, 130279; 45 C.F.R. §§ 164.302, 164.306, 164.308,164.310(b)

§126074 Security Requirements – Physical Controls

(a) Mobile Electronic Device Controls. A Demonstration Project Participant shall limit and protect any storage of IHI on mobile electronic computing devices and passive storage media. A Demonstration Project Participant shall limit and protect any storage of IHI on mobile electronic computing devices and passive storage media. A Demonstration Project Participant shall have a policy directing all workforce members, using entity-issued or any non-managed (user-owned) devices or media, to adhere to the entity mobile electronic computing device requirements. Storage of IHI on mobile computing devices and passive storage media is prohibited unless the devices or IHI:

(1) Are encrypted where indicated by risk assessment, and

(2) Legacy medical devices may require alternative controls in lieu of standard controls as allowed by device manufacturers, such deviations from standard controls shall be documented.

Authority: California Health and Safety Code §§ 130277, 130278.

Reference: California Civil Code§§ 1798.21, 1798.81.5; Health and Safety Code §§1280.15, 130200, 130277, 130279; 45 C.F.R. § 164.308(a)(7)

§126076 Security Requirements – Technical Controls

(a) Email & Messaging Security. A Demonstration Project Participant shall safeguard electronic mail and other messaging transmissions containing IHI through the use of encryption or an equivalent mechanism

(b) Audit Controls. A Demonstration Project Participant shall implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use IHI. The audit log parameters listed below are required for Demonstration Project Participants:

- Login ID (successful and unsuccessful attempts)
- Events (create, read, update, delete)
- Timestamp (date, time)
- Role (e.g. doctor, nurse, admin, billing, IT)
- Unauthorized accesses

(c) Consistent Time. A Demonstration Project Participant shall take steps to ensure clocks of all relevant information processing systems within an organization are synchronized using an accurate reference time source using the Network Time Protocol (NTP).

(d) Data Assurance. A Demonstration Project Participant shall protect IHI from unauthorized alteration or destruction. A Demonstration Project Participant shall implement technical security measures to guard against unauthorized access to, or modification of, IHI that is being transmitted over an electronic communications network.

(1) Encryption & Cryptographic Controls. A Demonstration Project Participant shall utilize encryption to the level appropriate to the data being protected, and where appropriate, to protect IHI. Demonstration Project Participants shall utilize the NIST Cryptographic Module Validation Program (CMVP) as the authoritative source of which products, modules, and modes are approved for use by NIST for Federal information Processing. This list, or its successor, should be periodically reviewed for updated information as part of each Demonstration Project Participant's internal best practices.

Authority: California Health and Safety Code §§ 130277, 130278.

Reference: California Civil Code§§ 1798.21, 1798.81.5; Health and Safety Code §§ 1280.15, 130200, 130277, 130279; 45 C.F.R. § 164.306(a), 164.308(a)(5),164.310, 164.312.

§126090 Demonstration Projects Oversight

(a) During the demonstration project, authorized CalOHII representatives may audit Demonstration Project Participants for compliance with these regulations, applicable state and federal law for the protection of individual privacy and the confidentiality of electronic health records with appropriate notice to the Demonstration Project Participant. An audit may include, but is not limited to inspection of:

(1) Privacy and security policies and procedures

(2) Adequacy of the consent informing process

(3) Training documentation

(4) Business associate agreements

(5) Participant Agreements

(6) Operations of the demonstration project, including impact of demonstration of alternative requirements.

(b) The Demonstration Project Participant must provide CalOHII with any and all requested documentation pertaining to 126090(a) within 10 business days of the receipt of the request or other time frame negotiated by the parties.

(c) CalOHII may conduct a site visit to observe operations of the demonstration project and compliance with these regulations.

(d) If CalOHII determines a Demonstration Project Participant is not in compliance with these regulations, a notice of non-compliance will be issued.

(1) A Demonstration Project Participant receiving a notice of non-compliance shall submit a plan of correction to CalOHII within 10 business days of the receipt of the notice of non-compliance.

(A) If CalOHII determines the plan of correction does not adequately address the identified instances of non-compliance, it may reject the plan of correction and request a Demonstration Project Participant to modify the plan of correction and resubmit within 5 business days.

(2) CalOHII may terminate a Demonstration Project Participant from remaining in a demonstration project or may terminate a demonstration project in its entirety if:

(A) CalOHII determines a Demonstration Project Participant has not adequately addressed identified areas of non-compliance; or

(B) If the Demonstration Project Participant has not complied with an accepted plan of correction; or

(C) If the non-compliance with the regulations is so egregious as to imminently threaten the security or privacy of the health information held by the Demonstration Project Participant.

(3) In the event of a termination, termination of a Demonstration Project Participant or the demonstration project shall occur in an orderly fashion balancing patient

health and safety with any time constraints in the Participant's Agreements with their HIO or other data sharing arrangements.

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: Government Code§ 11180 et seq.; Health and Safety Code §§ 130200, 130277, 130279.